Warmups for #3:

1. If a polynomial \( g \in \mathbb{Z}_2[X] \) has degree \( n \), then \( \mathbb{Z}_2[X]/(g(X)) \) has exactly \( 2^n \) elements.

2. If a polynomial \( g \in \mathbb{Z}_2[X] \) can be factored \( g = h_1 h_2 \), where \( h_1 \) and \( h_2 \) are nonconstant polynomials in \( \mathbb{Z}_2[X] \), then \( \mathbb{Z}_2[X]/(g(X)) \) is not a field – not even an integral domain.

3. Construct a field \( \mathbb{F}_8 \) with exactly 8 elements, as a quotient \( \mathbb{Z}_2[X]/(g(X)) \) for some polynomial \( g \in \mathbb{Z}_2[X] \). You will have to choose \( g \) carefully. Choose your notation for the 8 elements of \( \mathbb{F}_8 \) in such a manner that either the addition operation or the multiplication operation is obvious from your notation; then give the table defining the other operation.†

4. Show that in each of the following, \( I \) is an ideal in \( R \), by finding a ring \( S \) and a ring homomorphism \( \phi: R \to S \) whose kernel is exactly \( I \). (Do not verify the defining conditions for \( I \) to be an ideal.
You can’t use \( S = R/I \) because you don’t know yet that \( I \) is an ideal. Don’t try to “reconstruct” \( R/I \) in sneaky fashion; choose an appropriate ring \( S \) from the very familiar examples.)

(a) \( R = \mathbb{Z}[X] \), and \( I = (X^2 + 9) \). (Hint: find an equation that the element \( \phi(X) \in S \) will have to satisfy, then think of a ring \( S \) containing such an element.)

(b) \( R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\} \), and \( I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in R \mid b \in \mathbb{R} \right\} \)

5. In the following list, each ring is isomorphic to exactly one other. Decide what the “couples” are, and prove your assertion, including a proof that they are not all isomorphic to one another.

(a) \( \mathbb{Q}[X]/(X^2) \) (b) \( \mathbb{Q}[X]/((X - 1)^2) \) (c) \( \mathbb{Q}[X]/(X^2 - 1) \) (d) \( \mathbb{Q} \times \mathbb{Q} \)

Some relevant questions to narrow down the possibilities for the couples might be: Do these rings have zero divisors? Nilpotent elements? Idempotents? Are all zero divisors/nilpotent elements multiples of one another? How many ideals does each one have?

†Here are some theorems and facts about finite fields, which mostly won’t help you, and which you can’t use, but are interesting: for any prime \( p > 0 \) and \( n \in \mathbb{N} \), there is a field \( \mathbb{F}_{p^n} \) or \( GF(p^n) \) with exactly \( p^n \) elements. It is unique up to isomorphism. (On the other hand, there is no field with 6 elements, and more generally, if \( m \) is an integer which is not some power of some prime, then there is no field with exactly \( m \) elements.) In \( \mathbb{F}_{p^n} \), \( p = 1 + 1 + \cdots + 1 = 0 \), and there is an \( p \) summands

element (not unique) \( u \) such that the nonzero elements of \( \mathbb{F}_{p^n} \) are \( u = u^1, u^2, \ldots, u^{p^n-1} = 1 \). Such an element \( u \) is called a primitive root in \( \mathbb{F}_{p^n} \). For instance, \([3]_7 \) is a primitive root in \( \mathbb{Z}_7 \), but \([2]_7 \) is not (as \( 2^3 \equiv 1 \) (mod 7), the powers of \( [2]_7 \) give only 3 distinct elements). In \( \mathbb{Z}_5 \), there are two primitive roots: \([2]_5 \) and \([3]_5 \). Unless \( n = 1 \), the field \( \mathbb{F}_{p^n} \) cannot be described easily in terms of \( \mathbb{Z} \). In fact, the connection between addition and multiplication is so complicated and uninformative in some sense that cryptographers are fond of using fields with \( 2^n \) elements, \( n = 2, 3, 4, \ldots \), in the construction of encryption schemes. There is a significant body of research literature on finite fields, much of it from the last 50 years.